

文章编号:1001-9081(2008)06-1365-04

基于委托的分布式动态授权策略

张润莲^{1,2}, 武小年^{2,3}, 董小社¹

(1. 西安交通大学 电子与信息工程学院, 西安 710049; 2. 桂林电子科技大学 信息与通信学院, 广西 桂林 541004;

3. 现代通信国家重点实验室, 成都 610041)

(zhangrl@guet.edu.cn; xsdong@mail.xjtu.edu.cn)

摘要:针对分布式协作环境中的授权问题, 基于委托模型和 RBAC 模型, 提出一种基于委托的分布式动态授权策略。通过扩展 RBAC 模型的元素集和静态授权操作, 并由委托者动态创建临时委托角色和委托授权, 支持“部分角色转授权”。系统授权采用三级层次结构实现, 并给出了动态委托授权过程。系统实现及应用表明了其能够适应分布协作环境下的分布动态授权需求, 遵循“最小特权”原则。

关键词:访问控制; 委托授权; 角色访问控制; 公钥基础设施; 特权管理基础设施

中图分类号: TP393.08 **文献标志码:** A

Dynamic authorization scheme based on delegation in distributed system

ZHANG Run-lian^{1,2}, WU Xiao-nian^{2,3}, DONG Xiao-she¹

(1. School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an Shaanxi 710049, China;

2. School of Information and Communication, Guilin University of Electronic Technology, Guilin Guangxi 541004, China;

3. National Laboratory for Modern Communication, Chengdu Sichuan 610041, China)

Abstract: Concerning the authority in distributed environment for collaboration, a dynamic authorization scheme was presented based on delegation and RBAC model. The scheme supports partial role delegation, by expanding element sets of RBAC model, enlarging static authorization operations, and allowing the delegator to create temporary delegation roles and assign others (the delegatee) to the particular roles. The scheme was implemented by three-level frameworks, and the operating process about how to authorize dynamically in delegation model was described. The application shows that the scheme can adapt to distributed and dynamic environment, and follow the least privilege principle.

Key words: access control; delegation; Role-Based Access Control (RBAC); Public Key Infrastructure (PKI); Privilege Management Infrastructure (PMI)

0 引言

随着 Internet 的发展, 基于 Internet 的分布式计算也迅速发展, 出现了许多新的大规模、开放的分布式系统, 如网格计算、移动 Agent、多 Agent 系统等。在这种分布式环境中, 来自不同自治域的用户为协同工作, 如协同计算、联合科研等, 采用群组通信机制, 组成一个基于 Internet 的虚拟协作环境。由于组成员可以动态地加入、退出协作, 这种协作环境不仅要求有安全可靠的群组通信环境, 还要求有效地实施组内资源的访问控制, 提供安全的资源共享服务。多域协作环境的异构性和组成员的动态性, 需要分布式系统建立一种动态可扩展的授权和访问控制机制。

特权管理基础设施 (Privilege Management Infrastructure, PMI) 是 X.509v4 中提出的一种基于公钥认证的授权模型, 它将用户的属性信息保存在属性证书 (Attribute Certificate, AC) 中, 声明这个用户有什么权限, 什么属性, 能干什么^[1]。作为一种基础设施, PMI 最终目标是提供一种有效的体系结构来管理用户的特权属性, 进而对用户实施全面的授权服务。PMI 建立在公钥基础设施 (Public Key Infrastructure, PKI) 可信认证服务的基础上, 便于在分布式或系统结构呈多样性时进

行授权或委托授权。委托授权的基本思想是由管理者将其所具有的部分或全部权限转授给委托者, 让委托者代表其授权其他用户执行某些任务^[1]。通过委托授权, PMI 允许将分布环境下的集中式管理工作分散实施, 有效提高分布式系统的伸缩性。

为简化权限的分配、撤消操作, PMI 可通过属性证书支持角色访问控制 (Role-Based Access Control, RBAC)^[2]。基于角色的委托授权模型 (Role-based Delegation Model, RBDM) 是在 RBAC 基础上提出的一种旨在解决分布式环境下访问授权管理复杂性问题思想和安全机制。目前具有代表意义的 RBDM 模型主要有 RBDM0^[3] 和 RBDM2000^[4] 等, 但它们不支持权限级粒度的委托授权, 而是把角色作为委托授权的基本单位, 即只能委托角色及其所具有的全部特权, 这违背了 RBAC 策略中的“最小特权原则”, 使得用户可能会获得超出自身所需的权限许可, 从而造成信息安全隐患。尽管 PBDM (Permission-Based Delegation Model)^[5] 委托模型支持角色委托和部分委托, 但其同 RBDM2000 中的约束类似, 采用的是静态和粗粒度的约束, 在实际应用中存在不足。

针对分布协作环境中的授权问题, 本文根据委托模型和 RBAC 模型提出一种基于委托的分布式动态授权策略

收稿日期: 2007-12-25; 修回日期: 2008-03-03。 基金项目: 国家自然科学基金资助项目 (60773118); 国家 863 计划项目 (2006AA01A109); 现代通信国家重点实验室基金资助项目 (9140C1101050706)。

作者简介: 张润莲 (1974-), 女, 山西介休人, 博士研究生, 主要研究方向: 网格计算、信息安全; 武小年 (1972-), 男, 湖北监利人, 副教授, 硕士, 主要研究方向: 计算机网络信息安全、网络计算; 董小社 (1963-), 男, 陕西西安人, 教授, 博士生导师, 博士, 主要研究方向: 网络安全、信任管理、集群计算、网络计算。

(Dynamic Authority Scheme based on Delegation in Distributed system, DASDD)。DASDD 将 RBAC 模型中的角色集和用户集进行分类和扩展,并由委托者根据实际环境为组用户动态产生符合其职责能力的临时委托角色集并进行委托授权,支持“部分角色转授权”,实现分布环境下的动态授权;同时,通过细化的约束集对授权制约,避免不符合安全要求的权限转授和违反安全的权限冲突。

1 动态授权策略

为支持分布式动态授权,遵循“最小特权”原则,DASDD 将委托模型和 RBAC 模型相结合,通过分类和扩展 RBAC 模型元素集,为委托授权提供丰富的角色支持;并基于扩展的授权操作,允许委托者动态创建临时委托角色并委托授权。

1.1 DASDD 结构及基本元素集定义

DASDD 对 RBAC 模型中的角色集、用户集和约束集进行了分类和扩展,其结构如图 1 所示。

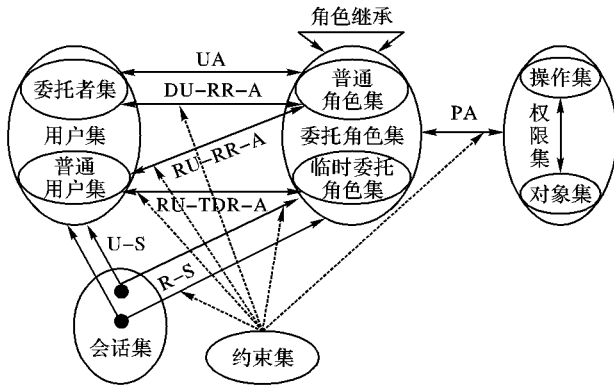


图 1 基于委托的动态授权结构

定义 1 DASDD 访问策略元素集。以 DASDD_RBAC 表示 DASDD 访问策略元素集。DASDD_RBAC = {OBS(资源对象集), OPS(访问操作集), PRMS(权限集), DR(委托角色集, Delegation Role), RR(普通角色集, Regular Role), TDR(临时委托角色集, Temporary Delegation Role), Users(用户集), DU(委托者集, Delegation User), RU(普通用户集, Regular User), Sessions(会话集), PA(权限-角色指派), UA(用户-角色指派), DU-RR-A(委托者-普通角色指派), RU-RR-A(普通用户-普通角色指派), RU-TDR-A(普通用户-临时委托角色指派), RH(角色继承), Constraints(约束集), U-S(用户-会话指派), R-S(角色-会话指派)}。其中: OBS、OPS、PRMS、Sessions、RH、PA、UA 与 NIST RBAC 模型中的定义一致,其他元素定义如下。

定义 2 用户集 User。用户集为分布式系统中所有用户所组成的集合,包括委托者集(DU)和普通用户集(RU),即 $User = DU \cup RU$ 。其中:

1) DU(委托者集)是所有具有委托授权能力的用户组成的集合,其从系统获得访问多域协作资源的访问许可,并能够为多域协作项目的组成员委托授权;

2) RU(普通用户集)是不具有委托授权能力的所有用户组成的集合,且 $DU \cap RU = \emptyset$ 。

通过将用户集分类,系统只需对委托者进行授权,普通用户则由委托者授权,大大减少了管理员的授权管理工作。根据分布多域协作的实际情况,每个协作项目可构成一个组,为简化概念,本文以委托者形成一个组并作为组管理员,其依据相关协作项目为组成员授权,使授权更灵活,易于表达实际需求。委托者也可在需要时设置具有二级委托能力的二级委托

者,这使授权工作被进一步分散实施,提高了分布式系统的伸缩性。同时,普通用户集可划分为具有不同资源访问能力的用户层次集合,如浏览者和执行者等,以建立相关的角色集。

定义 3 委托角色集 DR。DR 是所有角色的集合,可描述为 $assigned_permissions(r): DR \rightarrow 2^{PRMS}$,表示委托角色集与权限集间的映射关系;DR 包括普通角色集和临时委托角色集, $DR = RR \cup TDR$ 。

1) RR 是根据用户职责静态建立的普通角色集,可描述为 $assigned_permissions(r): RR \rightarrow DR \rightarrow 2^{PRMS'}$, $PRMS' \subseteq PRMS$,表示普通角色集与权限集间的映射关系;

2) TDR 是委托者根据实际场景需求动态建立的一种临时委托角色集,可描述为 $assigned_permissions(r): TDR \rightarrow DR \rightarrow 2^{PRMS'}$, $PRMS' \subseteq PRMS$,表示临时委托角色集与权限集间的映射关系。TDR 是已获得普通角色集的委托者授予组成员解决相关问题的最小能力, $TDR = R \cup P$,其中 $R \subseteq RR, P \in RR$ 。

在多域协作环境中,系统授权和权限撤销具有动态性和不可预知性,采用静态的授权策略难以适应其变化。本文扩展了委托者的能力,使其不仅可以进行委托授权,还具有创建角色的能力。以委托者自身所具有的普通角色集(RR)为基础,委托者可建立相适应的临时委托角色集(TDR),支持动态授权。将委托角色集分为普通角色集和临时委托角色集,并由不同人员创建,不仅简化了管理员的工作,且使得系统授权更加灵活,满足实际环境需求。

在创建 TDR 时,根据多域协作环境的实际情况,TDR 中的权限可能是委托者所获得角色或角色集的全部、也可能是某角色中的部分权限,从而可实现“部分角色转授权”的授权方式,遵循“最小特权”原则。TDR 之间也可通过继承关系,使得高级别的 TDR 继承低级别 TDR 的权限,方便委托者的委托操作。

1.2 DASDD 授权

DASDD 授权分为两部分:静态授权和动态委托授权。静态授权基于 RBAC 模型为 DASDD 的角色集等进行权限指派;动态委托授权将相关委托角色集委托授予某一用户。

定义 4 静态授权。静态授权可描述为一个五元组: $Assigned = (obs, p/r, r/u, du, c)$,其语义如下:委托者 du 依据所建立的约束集 c,将访问资源 obs 的权限 p 指派角色 r;或将访问资源 obs 的角色 r 授予用户 u。其中, $obs \in OBS, p \in PRMS, r \in DR, u \in User, du \in DU, c \in Constraints$ 。以 Assigned 分别表示 PA 和 UA 如下。

1) PA: $Assigned = (obs, p, r, du, c)$,其中, $obs \in OBS, p \in PRMS, r \in DR, du \in DU, c \in Constraints$ 。

2) UA: $Assigned = (obs, r, u, du, c)$,其中, $obs \in OBS, r \in DR, u \in User, du \in DU, c \in Constraints$ 。

通过限制角色或用户类型,可由 Assigned 表示权限-普通角色分配(P-RR-A)、权限-临时委托角色分配(P-TDR-A)、委托者-普通角色分配(DU-RR-A)、普通用户-普通角色分配(RU-RR-A)、普通用户-临时委托角色分配(RU-TDR-A),分别描述如下。

3) P-RR-A: $Assigned = (obs, p, r, du, c)$;其中, $obs \in OBS, p \in PRMS, r \in RR, du \in DU, c \in Constraints$ 。

4) P-TDR-A: $Assigned = (obs, p, r, du, c)$;其中, $obs \in OBS, p \in PRMS, r \in TDR, du \in DU, c \in Constraints$ 。

5) DU-RR-A: $Assigned = (obs, r, u, du, c)$;其中, $obs \in OBS, r \in RR, u \in DU, du \in DU, c \in Constraints$ 。

6) RU-RR-A: $Assigned = (obs, r, u, du, c)$; 其中, $obs \in OBS, r \in RR, u \in RU, du \in DU, c \in Constraints$ 。

7) RU-TDR-A: $Assigned = (obs, r, u, du, c)$; 其中, $obs \in OBS, r \in TDR, u \in RU, du \in DU, c \in Constraints$ 。

定义5 委托授权。委托授权通过签发属性证书(AC)实现。AC包含了证书持有者访问资源的能力,并具有一定的时效性。以一个五元组表示AC,则 $AC = (issuer, subject, tdr, delegation, constraints, timeinterval)$ 。其中, $(AC)_{issuer} \in DU$, 表示属性证书的签发者,即委托者。 $(AC)_{subject} \in User$, 表示属性证书的主体,即用户。 $(AC)_{subject, tdr} \subseteq DR$, 表示属性证书持有者 $(AC)_{subject}$ 所具有的角色集 tdr 。 $(AC)_{delegation}$ 表示委托步,即可以进行级联委托授权的次数或深度,其中, $delegation \in Z$ (Z 为整数), $delegation$ 依次减1,且当 $delegation = 0$ 时,所委托签发的AC无效。 $constraints \in Constraints$ 。以 $Time$ 表示时间集,以 $TimeInterval$ 表示时间区间集, $TimeInterval = Time \times Time$, $(AC)_{timeinterval} \in [t1, t2]$ 表示属性证书的有效时间间隔,其中, $t1, t2 \in Time$ 。若 $ac \in AC$, 则其语义为: 当且仅当委托者 $(AC)_{issuer}$ 为用户 $(AC)_{subject}$ 授予临时委托角色集 $(AC)_{subject, tdr}$ 的操作在满足委托约束条件 $constraints$ 且其委托深度 $(AC)_{delegation}$ 不超过规定值时是有效的,否则无效,且委托授予的权限有效时间维持在 $[t1, t2]$ 内。

通过静态授权的 P-TDR-A, 委托者可遵循“最小特权”原则, 建立符合用户职责能力且适应环境需求的临时委托角色集, 实现“部分角色转授权”; 而委托授权保证了系统能够在分布的多域协作环境中进行分布动态授权。

1.3 约束

为避免不符合安全要求的权限转授和违反安全的权限冲突, 在授权操作(包括静态授权和委托授权)过程需遵循特定的约束条件, 即在授权操作前进行限制检查, 只有被分配的主体(用户或权限)所在的角色中的当前成员或非成员满足约束条件才能执行操作。

定义6 冲突权限。在授权过程中, 不能够赋予同一个角色/用户的权限。用集合 CP 来定义冲突权限, $CP \subseteq PRMS \times PRMS$ 。对于一个权限 p , 定义与其冲突的权限集合为 $CP - with(p) = \{p_i | (p, p_i) \in CP \wedge p_i \in PRMS\}$ 。

定义7 冲突角色。在授权过程中, 不能够赋予同一个用户的角色。用集合 CR 来定义冲突角色, $CR \subseteq RR \times RR \cup TDR \times TDR \cup RR \times TDR$ 。对于一个角色 r , 定义与其冲突的角色集合为 $CR - with(r) = \{r_i | (r, r_i) \in CR \wedge (r_i \in RR \vee r_i \in TDR)\}$ 。

定义8 约束(Constraints)。约束是在 DASDD 的各种关系中起限制作用的一组制约集合。相关约束描述如下:

1) 在授权过程中, 冲突权限不能分配给同一个角色, 形式化描述为: $(p_i, p_j) \in CP \wedge (obs_i, p_i, r_i, du, c) \in Assigned \wedge (obs_i, p_j, r_j, du, c) \in Assigned \Rightarrow (r_i \neq r_j)$;

2) 在授权过程中, 冲突角色不能为同一个用户激活, 形式化描述为: $(r_i, r_j) \in CR \wedge (obs_i, r_i, u_i, du, c) \in Assigned \wedge (obs_i, r_j, u_j, du, c) \in Assigned \Rightarrow (u_i \neq u_j)$;

3) 权限缩减: 委托者不能为自己增加系统所授予的角色和权限之外的角色或权限, 其形式化描述为: $(obs, r, u, du, c) \in Assigned \Rightarrow u \neq du$;

4) 权限的有效性: 委托者在为用户授权时, 授予的角色和权限不能够超过其所拥有的角色和权限, 以 R 表示委托者 du 的角色和权限集, 其形式化描述为: $(obs, p_i/r_i, r/u, du, c) \in Assigned \Rightarrow p_i \in R \vee r_i \in R$ 。

2 DASDD 实现及应用

2.1 DASDD 实现

DASDD 的实现采用 Java 语言, 包括两个部分: 访问策略元素集管理和证书中心, 其实现框架如图2所示。

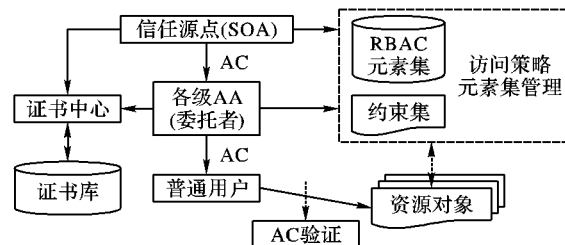


图2 DASDD 实现框架

1) 访问策略元素集管理。建立 DASDD 访问策略元素集, 包括资源对象集、操作集、权限集、委托角色集、用户集和约束集。约束集作为授权操作时的基本制约条件, 根据定义 6~8 将不同类型的约束采用不同的标识分别存储, 这使得系统在进行约束检验时提高查询效率。委托角色集中的普通角色集由管理员根据定义 1~4 建立, 临时委托角色由委托者根据实际情况动态创建并存储。上述元素集采用 Microsoft SQL Server 数据库存储管理。

2) 证书中心。完成对用户的授权和权限验证功能。系统授权的最终形式是为用户签发包含用户身份信息和访问权限的 AC。证书中心的实现基于 PKI^[6]/PMI^[1] 标准, 实现 AC 的申请、签发、维护和撤销, 并验证 AC 的有效性。为实现分布式授权, 证书中心为三级层次结构。最高层为信任源点(Source Of Authority, SOA), 是整个授权系统的最终信任源, 它负责系统安全规则的制定、各级 AA(Attribute Authority) 的设立审核, 并为各级 AA 签发具有委托能力的 AC, 相当于 PKI 中的根 CA, 对整个系统权限分发负有最终责任。中间层次为各级 AA, 即委托者, 是授权管理体系的核心服务节点, 其主要实施本域中的委托授权, 在授权过程中, 各级 AA 先根据系统需要建立符合约束规则的临时委托角色, 以支持“部分角色转授权”, 遵循“最小特权”原则; 并为组成员签发包含临时委托角色的 AC。由委托者动态建立的临时委托角色与普通角色一同存储在访问策略元素集数据库中, 并以特殊标识与普通角色相区别。最低层为普通用户, 持有由各级 AA 所签发的 AC 并以 AC 访问资源。所有的 AC 和证书撤销列表存储在证书库中。

2.2 动态委托授权实现过程

在分布式环境中, 为了确保多域协作中的信息安全, 采用上述策略进行委托授权还需要 PKI 支持。基于 Globus 中的安全组件 Java CoG Kit^[7] 和 PKI 标准^[6], 在各安全域中建立了 PKI 证书中心, 并为各用户和服务器签发了进行身份认证的公钥证书(Public Key Certificate, PKC)。在此基础上, DASDD 动态委托授权的实现过程如图3所示。

在图3中, 委托者在委托授权前先申请 PKC, 并以其 PKC 请求 SOA 授权。SOA 根据委托者 PKC 为委托者签发具有委托能力且包含了相关角色集的 AC。

为实现属性证书匿名授权, 委托者需要为组成员产生单次授权密钥对(One-Task Authorization Key, OTAK), 并产生密钥绑定证书(Key Binding Certificate, KBC)。OTAK 作为一次访问任务中用户的唯一标识, 可以替代用户身份认证密钥(包含在 PKC 中)作为授权认证密钥。KBC 证书通过绑定 OTAK 公钥和 PKC 公钥使得授权认证密钥独立于身份认证密

钥。基于对组员的签名(包括对该成员相关的 PKC 标识、KBC 公钥、OTAK 公钥和访问请求进行的签名),委托者为组成员签发含有临时委托角色信息的 AC。这样,证书中心通过对组成员 AC 的验证,可实现安全认证和权限验证。

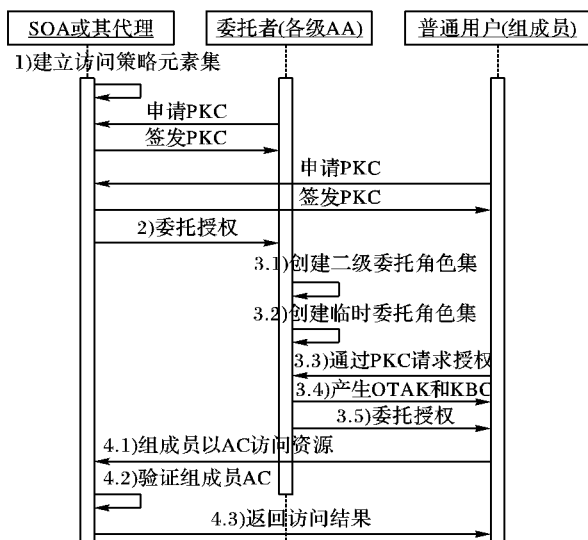


图3 DASDD 动态委托授权的顺序图

2.3 DASDD 应用

下面以 DASDD 在校园网络项目子系统教务管理系统中的应用进行说明。教学工作是一个由多个分布的教学部门协同完成的工作,其课程和教学人员众多,职责分工变化大,传统的授权机制难以满足系统需求。采用 DASDD 实现校园网络子系统教务管理系统的系统授权结构如图 4 所示。

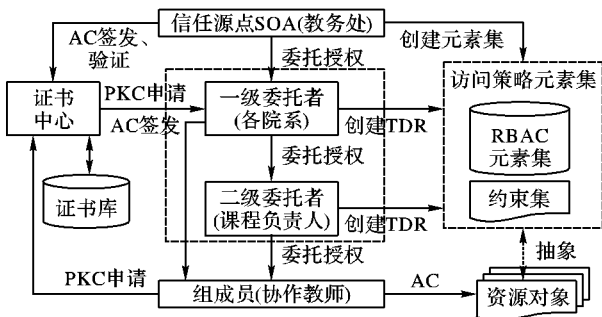


图4 DASDD 应用

如图 4 所示,根据教学工作职责划分授权层次:教务处作为系统授权的信任源点 SOA;各院系作为委托授权的核心服务点,建立各级 AA,即委托者(一级委托者);每门课程的主讲教师或课程负责人将作为二级委托者;其他协助主讲教师或课程负责人开展工作的教师则作为委托者的组成员(即普通用户)。教务处建立访问策略基本元素集,为各院系(一级委托者)授权。委托者根据协作项目的实际情况,动态创建临时委托角色集,为组成员授权。临时委托角色集被设置特定标识,可方便地撤销或转储,以适应授权的动态性。

委托者和组成员从校园网络 PKI 证书中心申请 PKC 证书,并依据 PKC 证书申请 AC。DASDD 基于 PKC 证书进行委托授权,为组成员产生 AC。组成员采用 AC 访问资源,此时,AC 不仅可以替代组成员的 PKC 证书进行安全认证,也包含了组成员访问资源的权限集。学期结束后,除委托者(包括一级和二级委托者)的能力外,组成员的能力将被撤销(AC 失效),一级委托者也可撤销发生变化的二级委托者的能力。

基于同样环境的教务管理系统,对比测试了采用 DASDD 进行认证与权限验证,和现有许多分布式系统中采用以 PKC

证书认证结合传统访问控制方法进行权限验证(以 DASDD 所建立的访问策略元素集进行传统权限验证)的性能开销,其结果如图 5 所示。测试结果表明,采用 DASDD 认证与权限验证的开销小于采用 PKC 证书认证结合传统权限验证的开销,其改善了系统性能。

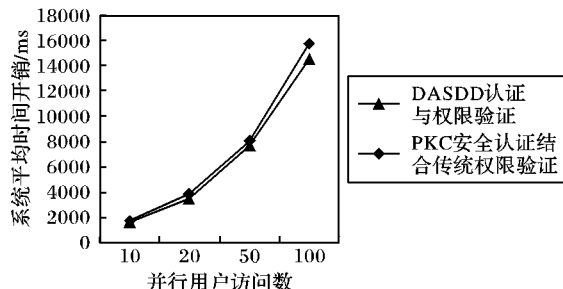


图5 DASDD 实现性能测试

DASDD 通过委托者创建临时委托角色并进行委托授权,不仅支持校园网络教务管理系统中各教学单位多域协作的分布、动态授权,也支持“部分角色转授权”,遵循了“最小特权”原则。系统增加了委托者的负担,但系统授权操作更加灵活。

3 结语

针对分布式协作环境中的授权和访问控制问题,本文基于委托模型和 RBAC 模型,提出一种基于委托的分布式动态授权策略。根据分布环境下多域协作的实际需要,分类和扩展了访问策略元素集和授权操作。系统采用三级授权层次结构,由委托者创建临时委托角色和委托授权,支持“部分角色转授权”。系统实现能够满足分布式协作环境中的分布、动态变化和安全管理需求。

参考文献:

- [1] CHADWICK D W. The X.509 privilege management infrastructure [C]// Proceedings of the NATO Advanced Networking Workshop on Advanced Security Technologies in Networking. Bled, Slovenia, 2003 [2007-10-03]. <http://www.cs.kent.ac.uk/pubs/2004/2278/content.pdf>.
- [2] FERRAILOLO D F, SANDHU R, GAVRILA S, et al. Proposed NIST standard for role-based access control [J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274.
- [3] BARKA E, SANDHU R. A role-based delegation model and some extensions [C]// Proceedings of the 23rd National Information Systems Security Conference (NISSC 2000). Baltimore, 2000 [2007-10-05]. <http://www.list.gmu.edu/confnrc/nissc/rbdlm00.pdf>.
- [4] BARKA E, SANDHU R. Role-based delegation model/ hierarchical roles (RBDM1) [C]// Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04). Washington: IEEE Press, 2004: 396-404.
- [5] ZHANG X W, OH S, SANDHU R S. PBDM: A flexible delegation model in RBAC [C]// Proceedings of the 8th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2003: 149-157.
- [6] TUECKE S, WELCH V, ENGERT D, et al. RFC 3820, Internet X.509 Public Key Infrastructure (PKI) proxy certificate profile [S/OL]. (2004-06) [2007-10-25]. <http://www.ietf.org/rfc/rfc3820.txt>.
- [7] Von LASZEWSKI G, FOSTER I, GAWOR J, et al. A Java commodity grid kit [J]. Concurrency and Computation: Practice and Experience, 2001, 13(8/9): 643-662.